UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 18-CIV-80176-Bloom/Reinhart

IRA KLEIMAN, as personal representative of
the estate of David Kleiman, and
W&K INFO DEFENSE RESEARCH, LLC,

Plaintiffs,

v.

CRAIG WRIGHT,

Defendant.
_______________________________________/

ORDER ON PLAINTIFF'S MOTION TO COMPEL (DE 210)

Encryption has existed as far back as the time of Julius Caeser.[1] The fundamental idea is simple: use a technique to hide something now, with a secret way to reveal it later. For text, the technique often involves a cipher – a way to encode the text itself. For physical objects, it generally involves creating a secure location that can only be entered using an access device, such as a key.

The modern world depends on encryption. Financial systems, national security, secure personal communications, and cloud storage all require encryption technology; otherwise they would be unprotected from hackers or intruders.

Modern cryptography is built on mathematics. The most famous cryptographic tool is the so-called "RSA" algorithm, which was developed by three MIT professors in 1977: Ron Rivest,

[1] Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, p. 9-10 (1999).

Adi Shamir, and Leonard Adleman.[2] The RSA algorithm is predicated on the computational difficulty of factoring the products of extremely large prime numbers.[3] In the RSA system, the encryption and decryption keys are numbers, specifically, integers.

On March 14, 2019, Dr. Wright was ordered to produce a list of his bitcoin holdings as of December 31, 2013. DE 124 at 18-23. On April 18, 2019, he filed a motion for protective order claiming that it would be unduly burdensome for him to produce the list. DE 155.[4] He claimed that he could not produce a complete list because, in or about 2010, he stopped keeping track of the public addresses (i.e., the unique identifiers) for the bitcoin that he mined.[5] He further stated, "In 2011, Dr. Wright transferred ownership of all of his Bitcoin into a blind trust." *Id.* at 2. He therefore claimed that he did not "know any of the public addresses which hold any of the bitcoin in the blind trust [and that he] cannot provide any other public addresses." *Id.*

The motion for protective order was denied. DE 166. Dr. Wright was further ordered to produce certain documents and certifications related to the trusts. Among the items he was ordered to produce were "all transactional records of the blind trust, including but not limited to any records reflecting the transfer of bitcoin into the blind trust in or about 2011." *Id.* at 4. This production was to be accompanied by a sworn declaration of authenticity. *Id.*

[2] *Id.* at 272-79.

[3] *Id.*

[4] The motion was filed under seal. A redacted version of the motion is filed in the public record at Docket Entry 184.

[5] Dr. Wright produced a partial list of bitcoin public addresses that he mined prior to 2011. DE 155 at 2-3.

Dr. Wright provided a sworn declaration dated May 8, 2019.[6] He swore that in October 2012 he settled a trust "whose corpus included the Bitcoin that I mined, acquired and would acquire in the future." Wright Declaration at ¶ 5.[7] He also swore, "Access to the encrypted file that contains the public addresses and their associated private keys to the Bitcoin that I mined, requires myself and a combination of trustees referenced in [the blind trust] to unlock based on a Shamir scheme." *Id.* at ¶ 23.

Plaintiffs move to compel Dr. Wright to comply with the Court's March 14 Order. They seek sanctions for his failure to do so. DE 197. Dr. Wright concedes that he has not complied with the Court's order, but argues that compliance is impossible. He expands upon the representation made in Paragraph 23 of his declaration. He argues that information necessary to produce a complete list of his bitcoin holding on December 31, 2011, is in the blind trust in an encrypted file that is further encrypted using "'Shamir's Secret Sharing Algorithm', an algorithm created by Adi Shamir to divide a secret, such as a private encryption key, into multiple parts." DE 204 at 5. Dr. Wright asserts that he cannot decrypt the outer level of encryption because he does not have all of the necessary decryption keys. *Id.* He states that after using a Shamir system to encrypt this information, "The key shares were then distributed to multiple individuals through the [blind] trusts" and "he alone does not have ability to access the encrypted file and data contained in it." *Id.*

[6] A copy of this declaration was emailed to the Court, but was not filed with the Clerk of the Court. Defendant shall file an unredacted version under seal forthwith and, after conferring with Plaintiffs, submit a proposed redacted version for filing in the public record.

[7] Dr. Wright now states that the bitcoin itself was not transferred to the trust. Rather, the private keys necessary to transfer the bitcoin were transferred to the trust, in an encrypted file.

A Shamir scheme is a technique for encrypting a piece of data.[8] Rather than securing the data with a single numerical key, multiple numerical keys are created. No single key can unlock the data. Some minimum number of the keys are needed for decryption. If the keys are distributed to multiple people, no single person can unilaterally unlock the data.

The underlying math can be complicated, but the end result is not.[9] A Shamir scheme creates a virtual safe deposit box. What, after all, is a safe deposit box? It is a location where items are stored but that cannot be opened by a single key. As anyone who has utilized a bank safe deposit box knows, opening the box requires both the bank's key and the customer's key. The customer keeps her key, so the bank cannot get into the box alone. The bank keeps its key so that the customer (or someone who steals the customer's key) cannot get into the box alone. Both keys are needed to open the box.

Under Shamir's system, each "key" is an ordered pair of numbers. The person encrypting the data can create multiple keys, all of which are needed to "unlock" the encrypted data. Think of a safe deposit box with many keyholes, not just two. The underlying concept is the same. If you get enough of the keys, you can unlock the data.

Dr. Wright concedes that a list of his bitcoin holdings could be generated from the information in the encrypted file in the trust. DE 204 at 4 (the encrypted file contains, *inter alia*, "other data from which information about bitcoin mined after block 70 could be re-generated."). Dr. Wright voluntarily encrypted this information using a Shamir system. *Id.* at 5 (Dr. Wright "purposely set up a Shamir system."). His declaration indicates that he is aware of the other

[8] Adi Shamir, How to Share a Secret, Communications of the ACM, Vol 22, No. 11, Nov. 1979, at 612.

[9] The mathematics is polynomial interpolation over a finite field modulo *p*, where *p* is a prime number. *Id.* at 613.

individuals who possess decryption keys. Those individuals are trustees of Dr. Wright's blind trust. He has not explained why he cannot obtain, and has not obtained, the necessary keys from these third parties. At this point, the record before the Court fails to demonstrate that Dr. Wright cannot through reasonable diligence comply with the Court's March 14th Order. The Court will allow the parties to develop a full evidentiary record before it decides whether sanctions are warranted.

WHEREFORE, it is ordered that:

1. The Motion to Compel (DE 210) is **GRANTED**. On or before **June 17, 2019**, Dr. Wright shall produce a complete list of all bitcoin he mined prior to December 31, 2013.

2. Dr. Wright shall appear in person before the undersigned at the Paul G. Rogers Federal Building, 701 Clematis Street, West Palm Beach, Florida, on **June 28, 2019 at 9:00 a.m.** to show cause why the undersigned should not certify the facts recited above to the Hon. Beth Bloom and order Dr. Wright to appear before Judge Bloom to show cause why he should not be adjudged in civil and/or criminal contempt by reason of these facts. 28 U.S.C. § 636(e)(6)(B) (2019).

3. At the June 28, 2019, hearing, the Court also will determine whether, independently, sanctions short of contempt should be imposed under Fed. R. Civ. P. 37 for Dr. Wright's failure to comply with the Court's March 14, 2019, Order.

DONE AND ORDERED in Chambers this 14th day of June, 2019, at West Palm Beach in the Southern District of Florida.

Bruce Reinhart

BRUCE REINHART
UNITED STATES MAGISTRATE JUDGE